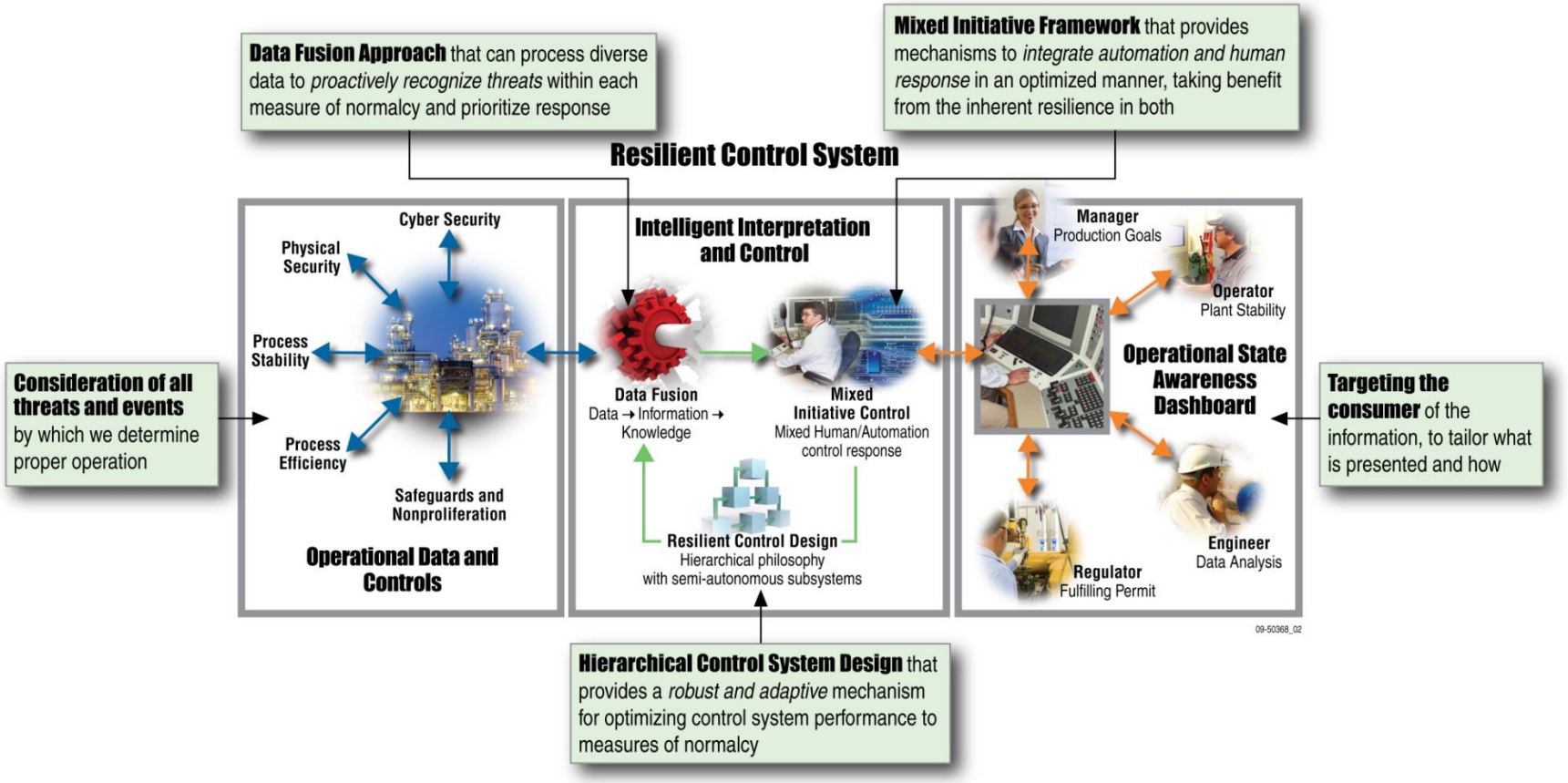
ISRCS 2010

www.inl.gov/isrcs

Notional Examples and Benchmark Aspects Of a Resilient Control System

Craig Rieger, PhD, PE

Resilient Control System Framework



Resilience and Current Research Philosophies

- **Current research philosophies do not take a holistic approach**
  - Cyber security research is immature and dependable computing research does not consider the unique design of a control system
  - Neither fault tolerant or reconfigurable control research provides the comprehensive plan to maintain performance in the face of threats
  - Fault detection and diagnosis (FDD) research does not consider malicious action to undermine normal system behavior
- **Multidisciplinary research needs**
  - A higher level hierarchical methodology that fuses and prioritizes incoming information to ensure state awareness and optimize response is lacking
  - Human reliability research does not consider the human as a benefit to overall resilience and a basis to the level of automation coupled to human performance
- **What follows:**
  - A characterization of current philosophy limitations
  - Notional examples to demonstrate
  - Resilience improvement recommendations

Unexpected Condition Adaptation

- ***Achievable hierarchy with semi-autonomous echelons***
  - The concept of cascading or supervisory control is not a new one, but in well-characterized applications or when few control loops are affected and can be brittle
  - Designers may lack full understanding of the interdependencies or made simplifying assumptions in regard to the loss of information
- ***Complex interdependencies and latency***
  - While the implementation of advanced control theory has been only gradual, the acceptance of digital technology is widespread
  - These systems are often designed and implemented in a local fashion, assuming facility stability will be achieved by the stabilization at the local level even though couplings can be complex
  - Concerns over the impacts of latencies on complex control algorithms have generated basic research involving the mitigation of these latencies

Human Interaction Challenges

- ***Human performance prediction***
  - While traditional concerns were often specific to ensuring correct judgment through the appropriate presentation of information
  - A more comprehensive interest involves measuring operator effectiveness for multiple control system interactions.
  - Unlike traditional design, a human contribution to resilience can be beneficial or detrimental.
- ***Cyber awareness and the intelligent adversary***
  - To focus specifically on those that understand security overlooks the fact that other work disciplines are also responsible for security off the control system operation
  - In addition, designs that require more passwords to enhance layered security protection, has diminishing benefit because of individual performance to implement consistently
  - Research and development to date has investigated better mechanisms to detect attacks, understanding attack vectors, and developing threat models
  - To provide measureable improvement in this design, one must reduce the overall complexity of implementing and maintaining the security protections.

Goal Conflicts

- ***Multiple performance measures***
  - Performance of control systems is based upon several measures, not just process stability, but also physical and cyber security, process efficiency, and process compliancy.
  - Such a philosophy, or measurement of the capacity remaining in the system before failure, is required and must be based on each measure of performance.
  - As these measures are also not considered in a holistic manner, fulfillment of overall performance or determination of priority can elude both the designers and the operators
  - Without a mechanism to consider heat sinks and sources within facilities, it is unrealistic to assume that the optimum efficiency is reached, or even known.
- ***Lack of state awareness***
  - Adding to multiple measures of performance, maintaining observability on conditions that characterize a shift from normal must also be achieved
  - While research in the areas of prognostics and fault diagnosis have been researched for over two decades, very little of this technology has engendered itself into a control system design
  - An observer for an unmeasured variable provides a useful analogy, but does not encompass what is effectively a separate discipline that uses multiple techniques to assess system condition
  - When considering measures such as cyber security, these technologies have not been applied, and in general, the field of cyber security metrics is in its infancy

Examples

- **Notional examples are developed to illustrate the limitations of current research philosophies in addressing the need:**
  - Power transmission substation
  - Chemical facility reactor
  - Heating, ventilation, and air conditioning (HVAC) system for a hazardous facility
- **Definitions:**
  - Operator/Dispatcher – the individual with direct responsibility for monitoring plant condition and making appropriate changes to maintain normal operation
  - Designer – the individual who develops the control system theory of operation
  - Adaptive capacity – may be used to describe the allowable loss in system functionality before a loss of acceptable performance is recognized

Power Transmission Substation Scenario

- **A transmission substation is interfaced to a SCADA System**
  - The communications to each relay is over an Internet Protocol (IP) based network
  - Uses standard Information Technology (IT) routing and segmenting equipment
  - Substation located in a building, with a locked door and surrounding fence with a locked gate
  - Inspection visits to the substation occur infrequently and normally only for maintenance
- **Backshift dispatcher receives an open breaker indication**
  - The breaker status returns to the normal closed position in one scan cycle
  - Crew investigates finding the fence lock missing and the substation door unlocked
  - An open door status alarm should have been indicated back at the control center
  - The breaker with the suspect condition is still closed and operating correctly
  - As substation appears undisturbed, other than the fence lock, there is no further investigation
- **Different crew is on the backshift a week later, when power is lost**
  - Numerous calls that the neighboring city has lost power, but no indication in the control center
  - Crew is dispatched to the substation that had been inspected the week before
  - Substation locks are secure, previously investigated breaker is now open, as are several others
  - An overload condition on the transmission lines eventually tripped power
  - A foreign wireless communications device was found during an investigation by security

Chemical Facility Reactor Scenario

- **A chemical reactor operation automated with a state-of-the-art DCS**
  - The communications system is an IP based design, which interconnects all of the controllers
  - DCS system is isolated from business systems via standard IT devices
  - The DCS provides multivariable control of the reactor via an optimal control methodology
  - The sensors that provide the data for this multivariable design are interfaced to multiple redundant controllers based on proximity to the process equipment
- **During the operation, a failure of a group of sensors occurs**
  - Depending on the type of failure, this event may or may not be recognized and responded to by current research philosophies
  - If they fail outside of normally accepted high or low levels and generate an alarm, limitations in current research philosophies become apparent
  - This failure could be due to cyber attack specific to an OLE for Process Control (OPC) server or a wireless access point, or it could be due to software failing in an undesirable/unexpected manner

Hazardous Facility HVAC Scenario

- **Hazardous facility using a DCS for regulating building pressures**
  - Most hazardous areas maintained at the lowest pressure and normally occupied spaces at the highest, preventing the migration of hazardous substances
  - System design also uses supervisory control, in that a neural network design implements night-time setbacks increases the air conditioning set points to reduce overall energy usage
  - Primary temperature and differential pressure control use a PID algorithm, with each hazardous zone having a controller and separate temperature controllers for hazardous and occupied zones
- **During early morning, exhaust largely blocked by damper failure**
  - This creates a back pressure on both the hazardous and occupied zones of the facility
  - In response to the reduced airflow, the inlet damper of each hazardous zone closes to maintain the required differential pressure
  - However, minimum facility flows are not maintained and the damper controls are not able to equalize consistently, allowing periods where potential migration of hazardous species may occur
  - As the airflow through the air conditioning coils has dropped, the PID controller continues to increase the amount of coolant to the coils until they freeze
  - As the occupied period is reached, the neural network decreases the temperature set points without regard to the abnormal situation and being outside the training regime of the neural network

Limitations: Power Transmission Substation

- **Unexpected Condition Adaptation**
  - Cyber compromise created a situation where overloading of the system is possible without the awareness of the centralized monitoring and control
  - The attacker can use readily available vendor software for configuring the relay settings to abnormally fault or not to bypass any intended equipment
- **Human Interaction Challenges**
  - A physical security alarm should have been recognized by the dispatcher at the control console, but these alarms can become a nuisance and ignored or turned off
  - The attacker bypassed the intrusion detection systems by attacking at the endpoint devices, and one connection allowed access to multiple devices
- **Goal Conflicts**
  - Operation of the power system and the cyber security of the system is a multidisciplinary responsibility
  - A status alarm from the substation door being opened would have provided some evidence of an impending compromise, but these alarms are considered low priority even when active

Limitations: Chemical Facility Reactor

- **Unexpected Condition Adaptation**
  - As the mechanisms of cyber attack are not characterized in current fault detection design and can result in corrupt data or latencies, this type of failure would be missed entirely
  - Timings specifically are crucial to an optimal control algorithm, and the failure of the sensors is from a cyber attack that injects latency, the control system may behave unexpectedly
- **Human Interaction Challenges**
  - As no alarms are expected, it would require a conscientious operator to determine process state changes in a timely fashion, which is also affected by the burden on the operator
  - Current cyber research philosophy does not consider the operator as a player in the cyber security response and there is a risk of undesirable responses being taken
- **Goal Conflicts**
  - The failure of the sensors can be due to many events; in this case, a software failure or cyber attack that causes the sensor to fail in a normal range
  - With the failures unknown to the operator, the operator can be lead to correct a perceived operational problem when a cyber failure is the cause

Limitations: Hazardous Facility HVAC

- **Unexpected Condition Adaptation**
  - Independent operation, which worked well during normal operation and expected disturbances, failed when an unexpected event occurred
  - A comprehensive supervisory hierarchy would benefit this situation, but a method of diagnosis would be necessary to detect out of bounds operation such as occurred with the neural network
- **Human Interaction Challenges**
  - Designer awareness of potential failures and boundaries is necessary during the design of the control response, and when these are not fully characterized, a worse situation can occur
  - Even if the designer allows for manual control, in case the automation fails in some way, the system must be attended to enable a response and is often not with HVAC
- **Goal Conflicts**
  - The HVAC system design has two apparent operating goals, temperature and differential pressure; however, there is no overarching mechanism to ensure that one goal is maintained over the other
  - A clear mechanism to consider the two goals would allow for prioritization of the differential pressure versus the temperature goal
  - To enable the prioritization, however, fault diagnosis through direct measurement or analysis would be needed

Resilience: Power Transmission Substation

- **Multi-agent designs for multi-level autonomy and peer negotiation**
  - Dependence on a centralized control room and automation, which creates a dependence upon communication links, can be destroyed during natural disasters or cyber attack
  - What multi-agent design can prevent are rapid shifts in load as resources can be negotiated at the substation, depending on available assets
- **Cyber awareness not a independent aspect of control system design**
  - While a substation break-in was the entry point for the malicious device, other avenues (such as an employee's compromised thumb drive) can be used to develop holes in current security protections
  - It is clearly important to ensure designed protections and controls are not overridden by malicious changes
  - Fusion of door failures with cyber detection can characterize an event that requires notification and response
- **The ability to respond quickly based on state awareness of the conditions provides adaptive capacity to the control system**

Resilience: Chemical Facility Reactor

- **Data fusion framework needed to confirm full state awareness**
  - While traditional redundancy, even triple modular redundancy, can maintain sensor information, unexpected failures lead to difficulties in prediction
  - The analysis and prioritization of the data will provide a basis for response, and is necessary to discriminate between failures that are software/hardware related and cyber related
- **Blend of automation and human response needed**
  - If a cyber event occurs, there is little in the way of current automation measures that would restore this situation
  - For the operator, the knowledge that the failure is cyber related would prevent an inappropriate action, such as making set point adjustments for the operation
  - For the security engineer and network technicians, modifications to isolate the network path for the cyber attack will be part of an appropriate response
- **Data fusion system provides an automated “resilience” response to complement the traditional fault tolerance design**

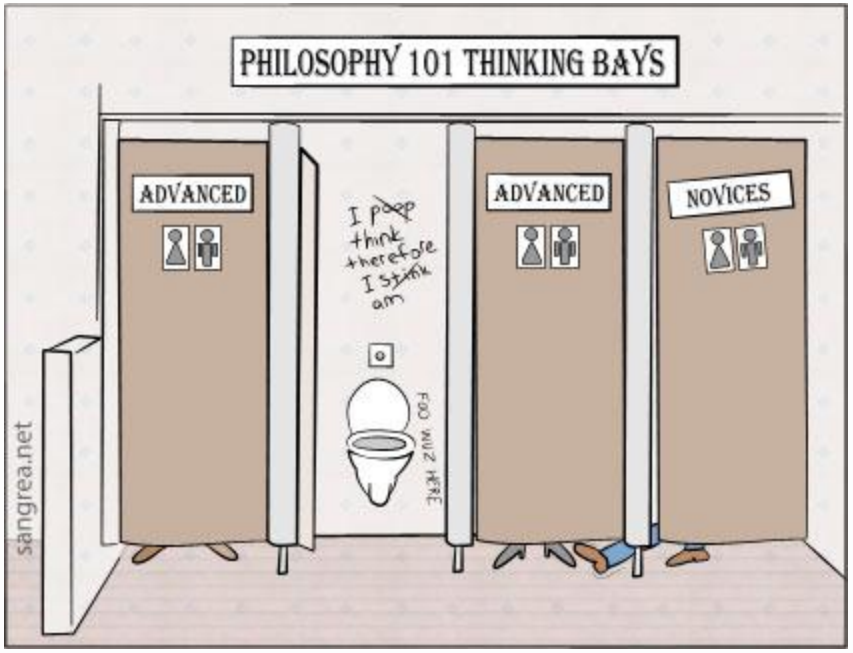
Resilience: Hazardous Facility HVAC

- **Hierarchical control methodology would have benefit**
  - Disconnection between differential pressure controllers and an overall operating philosophy, prevented adaptive capacity to be maintained while the controllers were reacting to the failure
  - Provide prioritization of the differential pressure vs temperature controls, and prevent reaction by the neural controller until the differential pressure had stabilized and the failure corrected
- **On-duty, trained operator could have partially mitigated this event**
  - Disengaging ineffective automation and giving similar preference to ensuring differential pressure on the most hazardous cells
- **An overall hierarchical strategy is necessary to improve the efficiency of the system and maintain prioritization of response**

Conclusions

- **Current research philosophies consider aspects of control system reliability, including reconfigurable control and cyber security**
  - However, limitations within these philosophies are exhibited in the area of goal conflicts, unexpected condition adaptation and human performance
  - In the case of the reconfigurable control, for instance, some key assumptions are made, specifically that the failure is known
  - Without considering cyber security as a performance parameter in the design, there is little hope of ensuring an adequate response to cyber events
- **Human performance provides an aspect of control system performance that can be beneficial or detrimental**
  - The discipline of human factors has demonstrated the need for understanding the interaction of human performance so that predictive and desirable responses can be achieved
  - The knowledge, experience, and questioning attitude of an operator can provide the ability to adapt to abnormal circumstances
  - The operator is not currently considered a stakeholder in cyber security, but their choice to delay response, in itself, can prevent the worst circumstances from being propagated.
- **The concept of resilient control systems cover many discipline areas, which are necessary to make a holistic approach to design**

QUESTIONS?


PHILOSOPHY 101 THINKING BAYS
ADVANCED
I poop think therefore I stink am
ADVANCED
NOVICES
FOO WUZ HERE
sangrea.net